El estado de la seguridad de la nube en Europa | 2022

La transición hacia Zero Trust

30 YEARS ANNIVERSARY

techconsult

TECHNOLOGY MARKET ANALYSTS

Table des matières

Avant-propos 2
Comment les entreprises protègent-elles leurs environnements de cloud? 3
Les principales inquiétudes vis-à-vis du cloud 4
Quiconque ne protège pas son cloud devient la cible des cybercriminels 5
Les avantages du concept « Zero Trust » 8
Qu'est-ce qui empêche les entreprises d'avoir recours au concept « Zero Trust » ? 9
Conclusion 10
Plus d'informations 11

Introducción

Actualmente los entornos en la nube juegan un papel esencial en toda empresa. En particular, el aumento del trabajo a distancia hace imprescindible que se migren importantes cargas de trabajo a la nube y se den a los trabajadores la posibilidad de acceder a los procesos empresariales importantes desde cualquier lugar.

Sin embargo, por otro lado, los criminales cibernéticos también saben que las empresas migran a la nube sus datos importantes. Estos entornos en la nube están fuera del perímetro de protección de las empresas y suponen un gran riesgo si la seguridad es deficiente. Especialmente mediante el phishing, los ciberdelincuentes pueden lograr obtener datos reales de acceso a los entornos de la nube y causar daños en ellos.

Entonces, ¿cómo pueden las empresas proteger sus entornos de la nube de la ciberdelincuencia? ¿Qué preocupaciones tienen sobre la nube? ¿y si ya han sido víctimas de ataques? ¿En qué puede ayudar un planteamiento de seguridad moderno como Zero Trust a mejorar la seguridad de la nube?

Para responder a estas preguntas, encuestamos a 400 responsables de la toma de decisiones sobre el nivel de desarrollo de la seguridad en la nube, la frecuencia de los ataques a los entornos en la nube y las ventajas y desventajas de Zero Trust. Los participantes en el estudio provenían de empresas con más de 500 trabajadores, de todos los sectores en Alemania, Reino Unido, Francia, países escandinavos, Italia, España y Benelux.

Derechos de autor
Este estudio lo elaboró la empresa techconsult GmbH. Los datos y la información que contiene se han investigado a conciencia y con la mayor diligencia posible según principios científicos. Sin embargo, no se puede garantizar su integridad y exactitud. Todos los derechos sobre el contenido de este estudio recaen sobre techconsult GmbH. Las reproducciones, incluyendo extractos, solo están permitidas con el consentimiento por escrito de techconsult GmbH.

Descargo de responsabilidad
La reproducción de nombres comunes, nombres comerciales, denominaciones de productos, etc. en esta obra no justifica la suposición de que tales nombres deban considerarse libres en el sentido de la legislación de marcas registradas y de protección de marcas y, por tanto, puedan ser utilizados por cualquiera, incluso sin un etiquetado especial. Las referencias que se hacen en este estudio a cualquier producto, proceso o servicio comercial específico por su nombre comercial, marca registrada, designación del fabricante, etc., no implican en modo alguno favoritismo por parte de techconsult GmbH.

Cómo protegen las empresas sus entornos en la nube

Cada vez se migra más carga de trabajo a la nube. Sin embargo, también hay que garantizar la seguridad de la nube. Muchas empresas no se consideran inicialmente responsables de la seguridad de la nube por sí mismas. Pero esto es una falacia, porque el principio de responsabilidad compartida se aplica a los entornos de nube. Los proveedores de la nube son responsables de la seguridad de la misma, es decir, de toda la infraestructura sobre la que se ejecutan los servicios en la nube. Las empresas, por su parte, son responsables de la seguridad en la nube, por ejemplo de la gestión de los datos o también de las autorizaciones de acceso a la nube.

Actualmente, 6 de cada 10 empresas afirman que protegen sus entornos de nube con medidas de seguridad especialmente diseñadas. Los bancos y las compañías de seguros son claros pioneros en lo que respecta a la seguridad en la nube. Casi tres cuartas partes de los proveedores de servicios financieros ya cuentan con una estrategia propia que asegura específicamente los entornos en la nube y la cuarta parte restante está en fase de planificación.

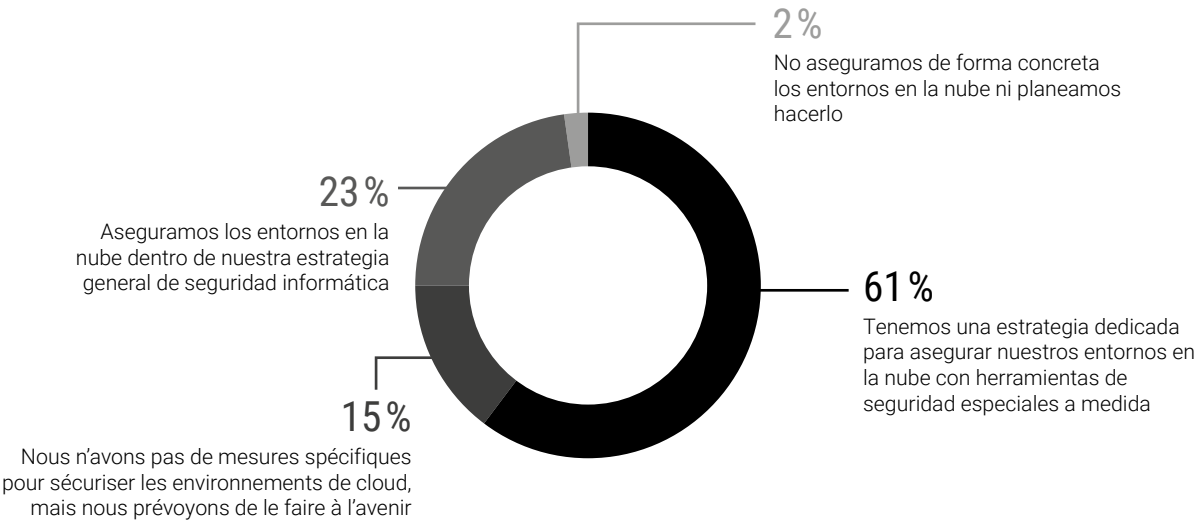
Aquí también entran en juego las estrictas reglas y normas que deben cumplir los proveedores de servicios financieros. Todas las demás empresas pueden tomar como ejemplo las medidas de seguridad de los proveedores de servicios financieros y adoptar las medidas adecuadas, incluso sin la normativa legal correspondiente.

En el 15 por ciento de las empresas no se ha implementado ninguna medida en la actualidad, pero tienen previsto introducir al menos medidas de seguridad específicas para los entornos en la nube en el futuro. Sin embargo, no se sabe exactamente cómo son estos planes ni en qué plazo de tiempo deberían llevarse a cabo. Esperar demasiado puede hacer que los propios entornos en la nube se conviertan en el objetivo de los ciberdelincuentes durante un periodo de tiempo más largo.

Los entornos en la nube están protegidos como parte de la estrategia general de seguridad informática en el 23% de las empresas. En este caso, cabe suponer que al menos prevalece una cierta protección básica. Sin embargo, si no se cumplen los requisitos individuales de seguridad en la nube con soluciones explícitas, la seguridad de los entornos en la nube no está garantizada.

¿Cómo de desarrollada cree que está su estrategia de seguridad en la nube?

Base: 400 empresas



Las mayores preocupaciones sobre la nube

La migración de las cargas de trabajo a la nube no solo tiene ventajas. Las empresas también se enfrentan a diversos riesgos de seguridad. Como parte de esta encuesta, los participantes pudieron seleccionar sus tres principales preocupaciones en cada caso.

El riesgo de seguridad más votado fue la caída general del servicio de la nube. No es de extrañar, porque un fallo del servicio en la nube también puede suponer la paralización de toda una empresa, dependiendo de la cantidad de cargas de trabajo que tengan lugar en la nube. También en este caso coinciden personas de todos los países en los que se realizó la encuesta: La interrupción del servicio en la nube fue elegida como el mayor riesgo en todos los países.

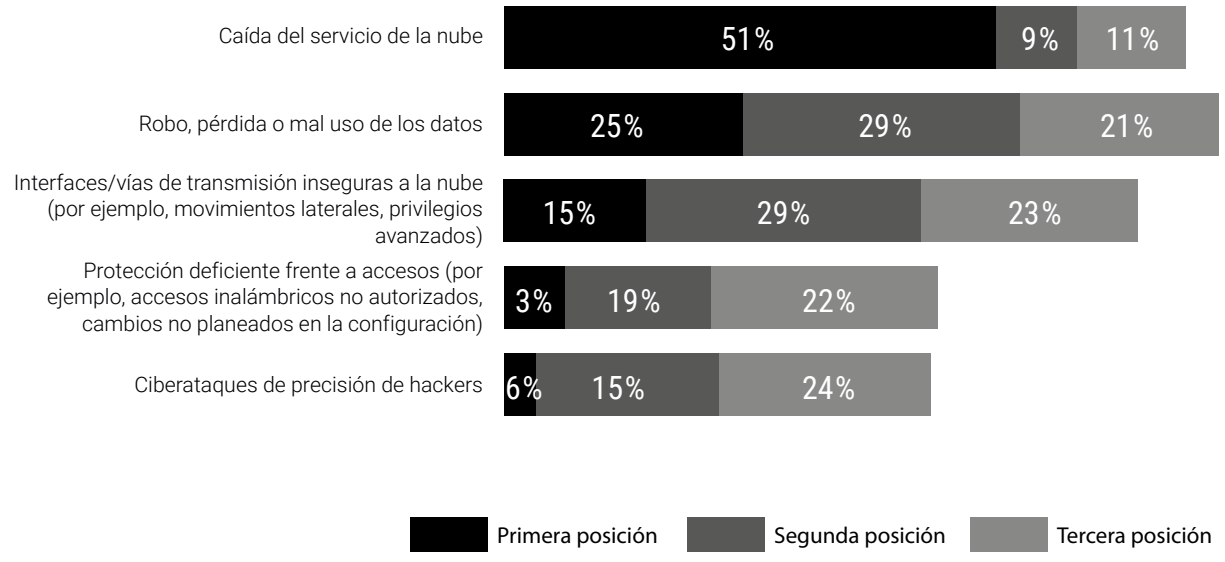
El miedo al robo, la pérdida y el mal uso de los datos fue votado en segundo lugar. En general, tres cuartos de los encuestados votaron riesgos que afectan a los datos en uno de los tres primeros lugares.

Los datos son un objetivo especialmente atractivo para los ciberdelincuentes, sobre todo en las empresas para las que el procesamiento de datos es una parte esencial de su negocio, y los datos críticos para el negocio que caen en manos equivocadas pueden ser fatales para una empresa.

Las interfaces inseguras o las vías de transmisión a la nube completan el top 3 de los mayores problemas de seguridad en torno a los entornos de nube. Especialmente debido al aumento del trabajo a distancia, cada vez más empresas recurren a la nube para gestionar sus procesos empresariales. Los ciberdelincuentes pueden utilizar la ingeniería social o los ataques man-in-the-middle para obtener las credenciales reales de un usuario. Este usuario comprometido puede convertirse rápidamente en un problema grave. Una vez que los atacantes han obtenido acceso a la red, también pueden adquirir privilegios adicionales y extenderse más y más profundamente en la red. A menudo pueden incluso hacerlo sin ser detectados, ya que sus movimientos en la red parecen el tráfico de red normal para las herramientas de seguridad tradicionales.

¿Cuáles cree que son los mayores riesgos para la seguridad en relación con los entornos en la nube?

Base: 400 empresas



Quiconque ne protège pas son cloud devient la cible des cybercriminels

Que los entornos en la nube son, efectivamente, el objetivo de los ciberdelincuentes y que las medidas para protegerlos son necesarias, lo demuestra la frecuencia de los ataques a la infraestructura en la nube. Un tercio de las empresas encuestadas afirma que al menos un ataque a sus entornos de nube tuvo éxito. En el 12% de las empresas, incluso se produjeron varios ataques con éxito. Sin embargo, el 42% de las empresas fueron capaces de detectar los ataques y rechazarlos.

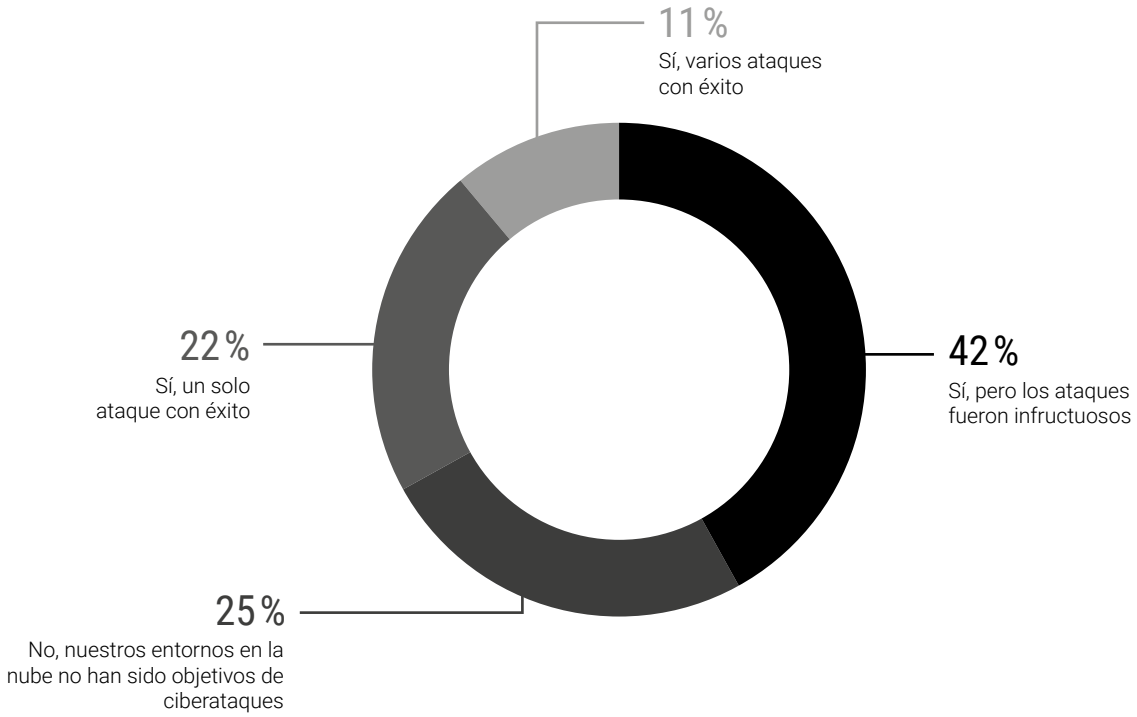
Las diferencias regionales en cuanto al éxito de los ciberataques en las empresas encuestadas son notables. Mientras que en Alemania, Italia y España algo menos de una cuarta parte ha sido víctima de la ciberdelincuencia al menos una vez, otras regiones se han visto afectadas por ciberataques con mucha más frecuencia.

Por ejemplo, el 38% de las empresas encuestadas del Reino Unido y el 40% de Francia fueron víctimas de ciberataques en entornos de nube. La situación es aún más grave para las empresas de la región nórdica y los países del Benelux. Aquí, incluso la mitad de las empresas han sido víctimas de un ciberataque con éxito al menos una vez.

Además, las empresas más grandes tenían menos probabilidades (20%) de haber sido víctimas de ataques exitosos que las empresas con menos de 5.000 empleados (37%). Esto sugiere que en las grandes empresas las medidas de seguridad son mucho más sofisticadas que en las pequeñas.

¿Han sido sus entornos en la nube ya objetivos de un ciberataque?

Base: 400 empresas



También es interesante: Las empresas que aún no protegen activamente sus entornos en la nube han sido víctimas de ciberataques con éxito con mucha más frecuencia que las empresas que protegen sus entornos en la nube, ya sea con la ayuda de una estrategia especial de seguridad en la nube o de forma rudimentaria como parte de una estrategia general de seguridad informática. Así, el 59% de las empresas que no tienen medidas especiales para asegurar la nube admitieron haber sido víctimas de ciberataques con éxito al menos una vez. En el caso de las empresas con seguridad en la nube propia, el porcentaje es solo del 31%. Esto lo deja claro: Las empresas que protegen sus entornos en la nube con medidas específicas tienen un riesgo menor que las que no tienen en cuenta la seguridad en la nube.

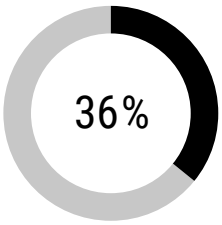
Para mejorar su propia seguridad informática y proteger también sus entornos de nube, las empresas pueden recurrir a un enfoque de Zero Trust. En este concepto de seguridad, no se confía en ningún dispositivo, usuario o servicio dentro o fuera de la red.

Se aplican amplias medidas para autenticar a todos los usuarios y servicios, y todo el tráfico de la red debe ser auditado. De este modo, las empresas reducen el riesgo de sus redes frente a las amenazas externas e internas. Los conceptos tradicionales de seguridad, en cambio, se centran en las amenazas externas y consideran que los usuarios y servicios internos son básicamente dignos de confianza.

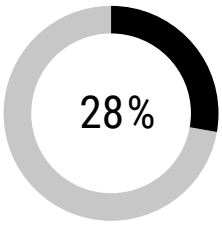
Hasta ahora, algo más de una cuarta parte de las empresas utilizan un modelo de Zero Trust. Los pioneros aquí son, una vez más, las instituciones del sector financiero o de seguros. Más del 40% de los proveedores de servicios financieros ya utilizan Zero Trust. Otro 40% se encuentra ya en la fase de aplicación concreta. Las empresas del sector minorista (20%) y las administraciones públicas (21%) pueden considerarse como claros rezagados.

¿Han implementado en su empresa ya un enfoque de «confianza cero» o planean implementar un modelo de este tipo en el futuro?

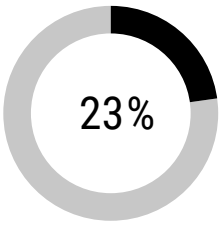
Base: 400 empresas



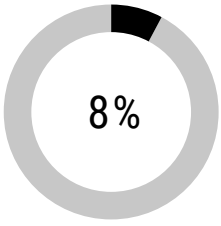
Sí, actualmente estamos en la fase de implementación



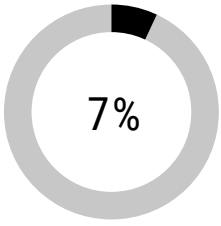
Sí, ya hay un enfoque de «confianza cero»



No, pero estamos en fase de planificación



No sabe / No contesta



No, tampoco planeamos un enfoque de este tipo

Zero Trust aún no está extendida en estos ámbitos, pero se desarrollará en el futuro. Casi el 46% de las empresas comerciales y el 33% de las administraciones públicas ya están aplicando Zero Trust. Solo hay algunas diferencias regionales. El grado de aplicación en todas las regiones se sitúa entre el 21% y el 28%.

Más de un tercio de las empresas están aplicando actualmente un enfoque de Zero Trust y otra quinta parte está al menos en la fase de planificación sin haber iniciado pasos concretos de aplicación. Esto demuestra claramente que Zero Trust se considera el concepto de seguridad del futuro en la mente de la mayoría de las empresas.

Especialmente las empresas que también tienen una estrategia para asegurar los entornos de la nube ya están más avanzadas en Zero Trust. El 38% de estas empresas ya utilizan Zero Trust, otro 38% están en proceso de introducir Zero Trust y el 15% están en fase de planificación. Esto significa que el número de empresas que utilizan Zero Trust superará el 90% en un futuro próximo, siempre que sigan sus anuncios con acciones.

En comparación, solo algo menos de una de cada ocho empresas sin protección especial en la nube utiliza un enfoque de Zero Trust. Sin embargo, se espera que la proporción aumente drásticamente en el futuro. Porque la implementación concreta de Zero Trust o la planificación general para su uso también está en pleno desarrollo en las empresas que aún no utilizan Zero Trust. Según sus propias declaraciones, más de tres cuartas partes de estas empresas se basarán en Zero Trust en el futuro.

Las ventajas de Zero Trust

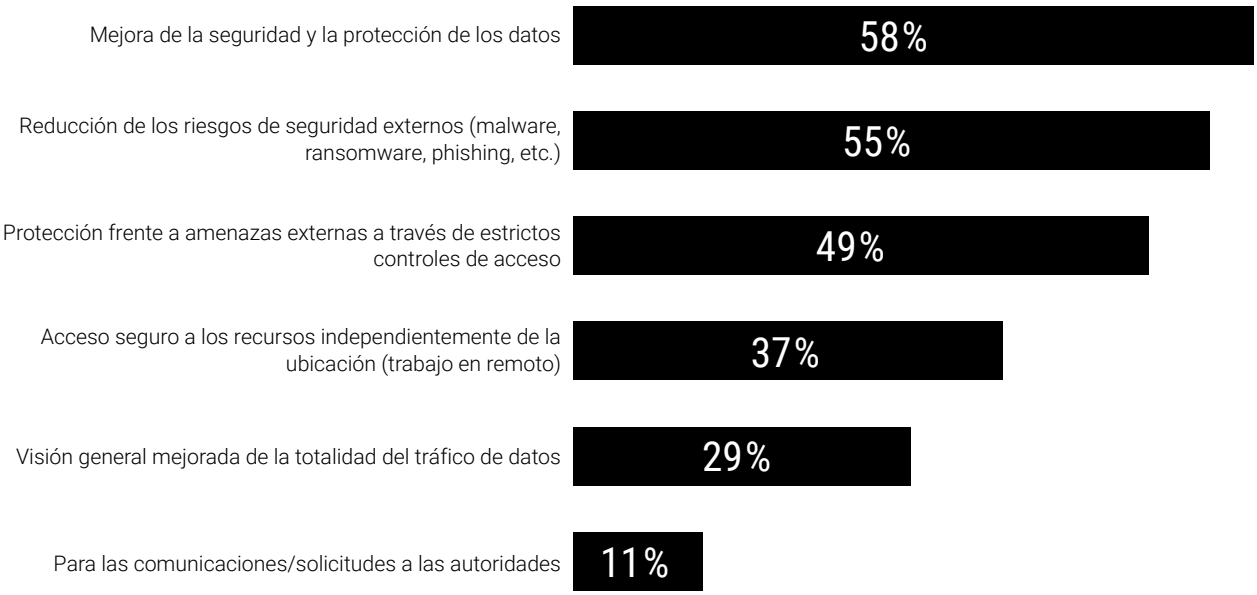
Protección de datos y reducción de riesgos externos e internos: estas son las tres principales ventajas que las empresas ven en Zero Trust. Especialmente en lo que respecta al creciente uso de la computación en nube, los conceptos de seguridad tradicionales no son del todo eficaces.

Seis de cada diez empresas consideran que la mejora de la seguridad y la protección de los datos es una de las principales razones para utilizar Zero Trust. Por ejemplo, en el modelo de Zero Trust, se analiza todo el tráfico y se pueden detectar intrusiones que pasarían desapercibidas con los enfoques tradicionales. Con los enfoques convencionales, los dispositivos se clasificarían como de confianza y podrían causar cualquier cantidad de daño dentro de las redes de la empresa. Con el modelo de Zero Trust, esto se evitaría desde el principio, minimizando así el riesgo de que los datos sensibles de la empresa caigan en manos equivocadas.

Le sigue la reducción de los riesgos de seguridad externos, como el malware, el ransomware o el phishing, con un 55%. El creciente número de ataques de phishing con éxito es una de las razones por las que las medidas de seguridad clásicas están perdiendo la batalla contra las ciberamenazas modernas. Esto se debe a que con las credenciales reales de los empleados, los ciberdelincuentes pueden, por ejemplo, burlar los controles de seguridad del correo electrónico y extenderse por la red. El enfoque de Zero Trust, en cambio, supondría que un remitente previamente autenticado puede verse comprometido en cualquier momento y lo comprueba de nuevo cada vez. Las actividades "no naturales" en la red se detectarían inmediatamente y el usuario sería aislado en consecuencia. Completando el top 3 está la protección frente a amenazas externas a través de estrictos controles de acceso (49%)..

¿Cuáles son los motivos decisivos para emplear un modelo de «confianza cero»?

Base: 343 empresas, enfoque de Zero Trust en vigor o previsto



¿Qué impide a las empresas utilizar Zero Trust?

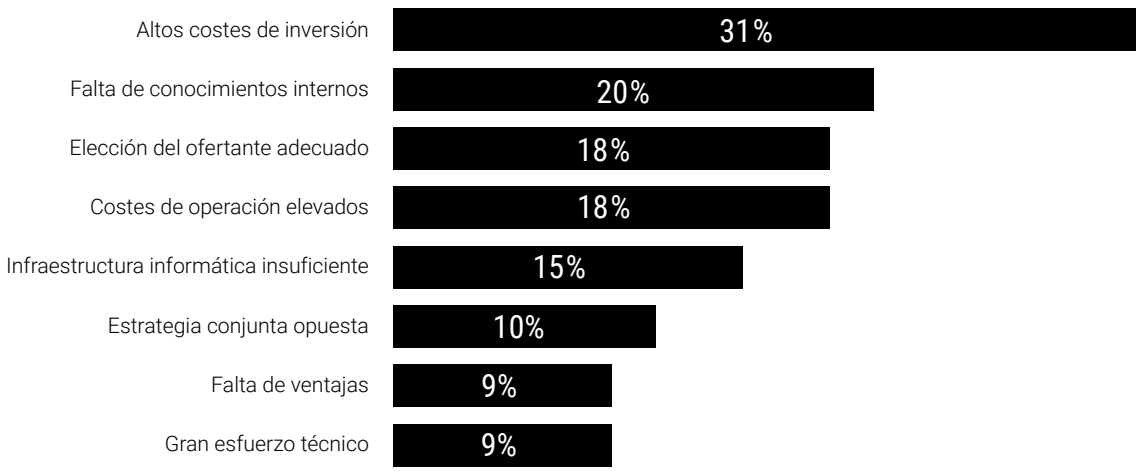
Las empresas que hasta ahora se han mostrado escépticas respecto a un enfoque de Zero Trust consideran que los altos costes de inversión suponen un gran problema. Casi un tercio de las empresas afectadas mencionaron este aspecto como una de las principales razones en contra de la introducción de Zero Trust. Sin embargo, Zero Trust no es un producto único que se instala, sino un enfoque estratégico en el que hay que analizar toda la organización y tomar las medidas de seguridad adecuadas. Por lo tanto, las inversiones en Zero Trust tienen un carácter estratégico que merece absolutamente la pena, porque los incidentes de seguridad y la pérdida de datos sensibles pesan mucho más, no solo monetariamente, sino también en términos de imagen.

A esto le sigue la falta de conocimientos en la empresa (20%) para aplicar Zero Trust.

Dado que Zero Trust no es un concepto de seguridad tradicional en el que simplemente se adquiere una única solución, sino un marco multidimensional de diferentes tecnologías, es necesario integrar Zero Trust en toda la empresa y transformar los procesos y estructuras existentes. Sin los conocimientos necesarios y la inclusión de todos los parámetros pertinentes, como las políticas de seguridad, la gestión de identidades, la clasificación de los datos o la ruptura de los silos, un enfoque de Zero Trust no puede tener éxito. Aquí es donde los proveedores especializados en Zero Trust ayudan a las empresas a implantarlo en toda la compañía. Sin embargo, el 18% de las empresas afirma tener problemas para elegir el proveedor adecuado. Por lo tanto, las empresas deben considerar de antemano cuál debe ser el objetivo de Zero Trust y cómo los proveedores pueden ayudar a alcanzarlo. También deben tenerse en cuenta las cuestiones relativas a la usabilidad, los modelos de implantación, los conocimientos específicos del sector o los socios tecnológicos.

"¿Qué motivos se opondrían a la introducción de la «confianza cero»?

Base: 55 empresas, no existe ni está previsto un enfoque de Zero Trust



Conclusión

Mientras que, por un lado, las empresas se benefician de las numerosas ventajas de la nube, los ciberdelincuentes ven un gran potencial para penetrar en las redes corporativas a través de entornos de nube no seguros y sus vías de acceso. De hecho, algo menos de un tercio de las empresas de los países encuestados en este estudio han sido víctimas de ataques dirigidos a sus entornos de nube al menos una vez. Por lo tanto, para protegerse eficazmente contra este tipo de ataques, las empresas deben asegurar los entornos de la nube con una estrategia de seguridad dedicada a ella y aplicar enfoques modernos dentro de la empresa.

Uno de estos enfoques es el de Zero Trust, en el que cada dispositivo y cada usuario se considera básicamente una fuente potencial de peligro y debe ser autenticado de nuevo cada vez. Las empresas que aplican este nuevo enfoque, que va mucho más allá de las soluciones de seguridad tradicionales, minimizan los posibles puntos de ataque para los ciberdelincuentes y reducen el impacto potencial general de los ataques exitosos.

Sin embargo, la implantación de Zero Trust no es una empresa sencilla; no se trata de una única herramienta de seguridad, sino de una estrategia holística para toda la empresa que analiza y transforma todos los procesos y estructuras. Por lo tanto, para implantar con éxito Zero Trust, es necesario abordar el proceso de transformación junto con un socio experimentado. Esta es la única manera de garantizar la máxima protección.

Más información

Pie de imprenta

techconsult GmbH
Baunsbergstraße 37
D-34131 Kassel

E-Mail: **info@techconsult.de**
Tel: +49 561 8109 0
Fax: +49 561 8109 101
Web: **www.techconsult.de**

Contacto para más información

Raphael Napieralski
Analista
E-Mail: **raphael.napieralski@techconsult.de**
Tel.: +49 561 8109 0

Acerca de techconsult GmbH

Techconsult GmbH, fundada en 1992, es una de las empresas de análisis establecidas en Europa Central. La consultoría estratégica se centra en las tecnologías de la información y la comunicación (TIC). A través de años de investigación estándar e individual, techconsult tiene un stock de información único en el mundo de habla alemana, tanto en términos de continuidad como de profundidad de la información, y por lo tanto es un importante socio de consultoría para los CXO, así como la industria de TI cuando se trata de la innovación de productos, la estrategia de marketing y el desarrollo de ventas.